

UNITED STATES DISTRICT COURT  
DISTRICT OF OREGON  
PORTLAND DIVISION

QUEST SOFTWARE, INC., a Delaware  
corporation,

Plaintiff,

v.

NIKE, INC., an Oregon corporation,

Defendant.

Case No.: 3:18-cv-00721 BR

**AGREEMENT REGARDING  
DISCOVERY OF  
ELECTRONICALLY STORED  
INFORMATION AND ORDER**

The parties hereby stipulate to the following provisions regarding the discovery of electronically stored information (“ESI”) in this matter:

**A. General Principles**

1. An attorney's zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

2. The proportionality standard set forth in Fed. R. Civ. P. 26(b)(1) must be applied in each case when formulating a discovery plan. To further the application of the proportionality standard in discovery, requests for production of ESI and related responses should be reasonably targeted, clear, and as specific as possible.

**B. ESI Disclosures**

The parties disclose the following information in Appendix A:

1. Custodians. The five custodians most likely to have discoverable ESI in their possession, custody or control. The custodians shall be identified by name, title, connection to the instant litigation, and the type of the information under his/her control.

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -1-

2. Non-custodial Data Sources. A list of non-custodial data sources (e.g. shared drives, servers, etc.), if any, likely to contain discoverable ESI.

3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain discoverable ESI (e.g. third-party email and/or mobile device providers, “cloud” storage, etc.) and, for each such source, the extent to which a party is (or is not) able to preserve information stored in the third-party data source.

4. Inaccessible Data. A list of data sources, if any, likely to contain discoverable ESI (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

5. ESI Liaison. Each party agrees to identify a person with the ability to facilitate the preservation, retrieval, and production of each party's ESI throughout the course of the litigation. This liaison may be a party to the action and must be available to participate in any discovery motion hearing involving ESI.

### **C. Preservation of ESI**

The parties acknowledge that they have a common law obligation to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody or control. With respect to preservation of ESI, the parties agree as follows:

1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody or control.

2. All parties shall supplement their disclosures in accordance with Fed. R. Civ. P. 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded under (C)(3) or (D)(1)-(2) below).

3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:

- a. Deleted, slack, fragmented, or other data only accessible by forensics.
- b. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.
- c. On-line access data such as temporary internet files, history, cache, cookies, and the like.
- d. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(5)).
- e. Back-up data that are substantially duplicative of data that are more accessible elsewhere.
- g. Data remaining from systems no longer in use that is unintelligible on the systems in use and where there is no reasonable way to convert the data to a universal format such as CSV, XLSX, TXT, SQL, XML, etc.
- h. Electronic data (e.g. email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), provided that a copy of all such electronic data is routinely saved elsewhere (such as on a server, laptop, desktop computer, or “cloud” storage).

#### **D. Privilege**

1. With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

2. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).

#### **E. ESI Discovery Procedures**

1. On-site inspection of electronic media. Such an inspection shall not be permitted absent a demonstration by the requesting party of specific need and good cause or by agreement of the parties.

2. Search methodology. The parties agree that in responding to any Fed. R. Civ. P. 34 request, or earlier if appropriate, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery.

The parties further agree that they will conduct good faith, reasonable searches for

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -3-

responsive material and information pursuant to their obligations under the Federal Rules of Civil Procedure and any applicable Local Rules.

3. Format. The parties agree that ESI will be produced to the requesting party with searchable text. The parties will produce ESI in single-page, black and white, TIFF Group IV, 300 DPI TIFF images with the exception of PowerPoint and spreadsheet type files, source code, audio, and video files, which shall be produced in native format. If an original document contains color that is used for emphasis, red-lining, highlighting, in charts, diagrams or photographs or that is otherwise necessary to understand the meaning or content of the document, the document should be produced as single-page, 300 DPI JPG images with JPG compression and a high quality setting as to not degrade the original image. Parties are under no obligation to enhance an image beyond how it was kept in the usual course of business. TIFFs/JPGs will show any and all text and images which would be visible to the reader using the native software that created the document. For example, TIFFs/JPGs of e-mail messages should include the BCC line. PowerPoint documents shall be processed with hidden slides and all speaker notes unhidden, and shall be processed to show both the slide and the speaker's notes on the TIFF/JPG image.

If a document is produced in native, a single-page Bates stamped image slip sheet stating the document has been produced in native format will also be provided. Each native file should be named according to the Bates number it has been assigned, and should be linked directly to its corresponding record in the load file using the NATIVELINK field. To the extent that either party believes that specific documents or classes of documents, not already identified within this protocol, should be produced in native format, the parties agree to meet and confer in good faith. Such documents shall have a one-page Bates numbered TIFF image placeholder with a corresponding native file. Document that are locked by a password or encrypted as they are kept in the ordinary course of business shall be produced in a form that is unlocked or decrypted.

Certain types of databases are dynamic in nature and will often contain information that is neither relevant nor reasonably calculated to lead to the discovery of admissible evidence. Thus, a party may opt to produce relevant and responsive information from databases in an alternate form, such as a report or data table. These reports or data tables will be produced in a static format.

The parties agree to identify the specific databases, by name, that contain the relevant and responsive information that parties produce.

4. De-duplication. The parties shall de-duplicate their ESI production across custodial and non-custodial data sources using MD5 hash, SHA1 hash, or other agreed upon de-duplication methods after disclosure to the requesting party.

5. Metadata fields. The parties agree to produce metadata fields contained in Appendix B. However, the parties are not obligated to produce metadata for any document that does not contain such metadata in the original, if it is not possible to automate the creation of metadata when the document is collected. The parties reserve their rights to object to any request for the creation of metadata for documents that do not contain metadata in the original.

All ESI will be produced with a delimited, database load file that contains the metadata fields listed in Appendix B, attached hereto, to the extent that such metadata fields exist, are maintained in the ordinary course of business, and can be automatically extracted from the electronic documents. The parties agree to make reasonable efforts to collect and produce accurate and complete metadata but the parties understand that due to how documents are created and stored, ESI may not include all of the metadata fields or that the metadata information may not always be accurate.

DATED this 7th day of February, 2019.

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -5-

WEST\284915843.1.1

**STOKES LAWRENCE, P.S.**  
1420 FIFTH AVENUE, SUITE 3000  
SEATTLE, WASHINGTON 98101-2393  
(206) 626-6000

STOKES LAWRENCE, P.S.

STOEL RIVES LLP

By: /s/ Bradford J. Axel

Thomas A. Lerner (OSB No. 804626)  
Bradford J. Axel (admitted *pro hac vice*)  
Elizabeth A. Findley (admitted *pro hac vice*)  
Theresa H. Wang (admitted *pro hac vice*)  
1420 Fifth Avenue, Suite 3000  
Seattle, Washington 98107  
Telephone: (206) 626-6000  
Facsimile: (206) 464-1496  
*tom.lerner@stokeslaw.com*  
*bradford.axel@stokeslaw.com*  
*elizabeth.findley@stokeslaw.com*  
*theresa.wang@stokeslaw.com*

Annette L. Hurst (admitted *pro hac vice*)  
Nathan Shaffer (admitted *pro hac vice*)  
ORRICK, HERRINGTON & SUTCLIFFE  
LLP  
405 Howard Street  
San Francisco, California 94105  
Telephone: (415) 773-5700  
Facsimile: (415) 773-5759  
*ahurst@orrick.com*  
*nshaffer@orrick.com*

Attorneys for Plaintiff Quest Software Inc.

By: /s/ B. John Casey

B. John Casey, OSB No. 120025  
760 SW Ninth Avenue, Suite 3000  
Portland, Oregon 97205  
Telephone: (503) 224-3380  
Facsimile: (503) 220-2480  
*john.casey@stoel.com*

Andrew L. Deutsch (admitted *pro hac vice*)  
DLA PIPER LLP  
2000 Avenue of Stars  
Los Angeles, California 90067  
Telephone: (310) 595-3000  
Facsimile: (310) 595-3030  
*andrew.deutsch@dlapiper.com*

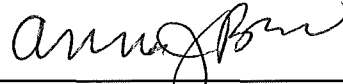
Francis W. Ryan (admitted *pro hac vice*)  
Kerry A. O'Neill (admitted *pro hac vice*)  
DLA PIPER LLP  
1251 Avenue of the Americas  
New York, New York 10020  
Telephone: (212) 335-4850  
Facsimile: (212) 335-4501  
*frank.ryan@dlapiper.com*  
*kerry.oneill@dlapiper.com*

Attorneys for Defendant Nike, Inc.

**ORDER**

Based on the foregoing, IT IS SO ORDERED.

DATED: 2/12/19



---

The Honorable Judge Anna J. Brown  
UNITED STATES SENIOR DISTRICT  
JUDGE

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -7-



**APPENDIX A**1. Custodians.

<b>Name</b>	<b>Title</b>	<b>Connection to the Instant Litigation</b>	<b>Type of Information Under Control</b>
Alan Akins	Global End User IT Asset Manager	Participated in diligence regarding Nike's response to Quest audit	IT Software Purchasing
Mike Wittig	VP, Infrastructure Engineering	Manages Nike employees who use Quest Software	IT Infrastructure
Randy Seale	Sr. Security Incident Responder / Corporate Information Security	Participated in diligence regarding Nike's response to Quest audit	IT Security
Kimberly King	IT Vendor Management Expert	Participated in diligence regarding Nike's response to Quest audit findings	IT Structure and Organization
Sandeep Bhargava	Director of Database, Storage and Backup Services	Oversees use of Quest Software in database administration	IT Structure and Organization

2. Non-custodial Data Sources. Nike utilizes shared drives and servers that may contain discoverable ESI. As set forth in paragraph E.2. of this Order, Nike will conduct good faith, reasonable searches for responsive material and information pursuant to their obligations under the Federal Rules of Civil Procedure and any applicable Local Rules.

3. Third-Party Data Sources. None.

4. Inaccessible Data.

- a. Internal Security Logs that are more than 400 days old. Nike keeps internal security logs which track logins, access, and other security data for users on the Nike network. Internal security logs older than 400 days are retained but kept in "cold storage." The retrieval of internal security logs from cold storage cannot be



achieved without great effort and expense and is thus not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

- b. Server Log information predating the server. Nike keeps “server log” information that can be used to track each Nike user who accessed Quest Software on a given server. Server log information is limited to the date on which the particular server was built or rebuilt. Thus, retrieving server log information from a given server predating the server's build or rebuild is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).

- 5. ESI Liaison. Nike designates Genardo Lopez (Director, Global Records Management) as its ESI Liaison.

**APPENDIX A**

1. Custodians:

a. a. Stephen (Field) Turner

- i. Title: National Account Manager.
- ii. Connection to Instant Litigation: Mr. Turner provided services and support related to the Nike account.
- iii. Type of Information Under His Control: Emails and user-generated documents, including those pertaining to the Nike account.

b. Eric Haslinger

- i. Title: North America Sales Director.
- ii. Connection to Instant Litigation: Mr. Haslinger managed the sales team that oversaw the Nike account.
- iii. Type of Information Under His Control: Emails and user-generated documents, including those pertaining to sales.

c. Megan Mentink

- i. Title: Technical Manager, License Compliance Operations.
- ii. Connection to Instant Litigation: Ms. Mentink participated in discussions regarding Quest's audit of Nike.
- iii. Type of Information Under Her Control: Emails and user-generated documents, including those pertaining to license compliance operations.

d. Josh Baker

- i. Title: Senior Manager, License Compliance.
- ii. Connection to Instant Litigation: Mr. Baker participated in audit lead-up and follow-up with Nike, as well as attempts at resolution.
- iii. Type of Information Under His Control: Emails and user-generated documents, including those pertaining to license compliance.

- e. Douglas Wakeman
  - i. Title: Contracts Manager.
  - ii. Connection to Instant Litigation: Mr. Wakeman managed aspects of Nike contracts and participated in contract language negotiation.
  - iii. Type of Information Under His Control: Emails and user-generated documents, including those pertaining to contract management and negotiation.
- 2. Non-custodial Data Sources: Quest maintains data that may include discoverable ESI on shared servers and drives. Quest will run searches for responsive data in accordance with its duty under the Federal Rules of Civil Procedure and the Local Rules.
- 3. Third-Party Data Sources:  
Deloitte, which conducted the audit of Nike, may have responsive documents. Dell Software, Quest Software's predecessor in interest, may also have retained responsive documents.
- 4. Inaccessible Data.  
Quest may not have access to certain institutional documents for the period of its ownership by Dell from approximately 2012 through 2016. Some employees remained employed for the duration of the organizational changes and therefore have documents from this time period. However, such documents may not have been transferred on any specific retention plan. Accordingly, Quest will produce any responsive documents it has from this time period, but notes that such documents were not routinely kept.
- 5. ESI Liaison.  
Richard Bradford, Director, Program Management & Business Analysis

**APPENDIX B**

Field Name	Example / Format	Description
<b>BEGNO</b>	ABC0000001 (Unique ID)	The Document ID number associated with the first page of a document.
<b>ENDNO</b>	ABC0000003 (Unique ID)	The Document ID number associated with the last page of a document.
<b>BEGATTACH</b>	ABC0000001 (Unique ID; Parent-Child Relationships)	The Document ID number associated with the first page of the parent document.
<b>ENDATTACH</b>	ABC0000008 (Unique ID; Parent-Child Relationships)	The Document associated with the last page of the last attachment.
<b>SENDATE</b>	MM/DD/YYYY	The date the e-mail or calendar entry was sent.
<b>SENTTIME</b>	HH:MM	The time the e-mail or calendar entry was sent.
<b>RECEIVEDDATE</b>	MM/DD/YYYY	The date the document was received.
<b>RECEIVEDTIME</b>	HH:MM	The time the document was received.
<b>AUTHOR</b>	jsmith	The author of a document from extracted metadata.
<b>LASTEDITEDBY</b>	jsmith	The name of the last person to edit the document from extracted metadata.
<b>FROM</b>	Joe Smith <jsmith@email.com>	The display name and e-mail address of the author of an e-mail/calendar item. An e-mail address should always be provided.
<b>TO</b>	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail address of the recipient(s) of an e-mail/calendar item. An e-mail address should always be provided for every e-mail if a recipient existed.
<b>CC</b>	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail of the copyee(s) of an e-mail/calendar item. An e-mail address should always be provided for every e-mail if a copyee existed.
<b>BCC</b>	Joe Smith <jsmith@email.com>; tjones@email.com	The display name and e-mail of the blind copyee(s) of an e-mail or calendar item. An e-mail address should always be

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -10-

		provided for every e-mail if a blind copyee existed.
<b>SUBJECT</b>		The subject line of the e-mail/calendar item.
<b>CUSTODIAN-ALL</b>	Smith, Joe; Doe, Jane	All of the custodians of a document from which the document originated, separated by semicolons.
<b>ATTACH COUNT</b>	Numeric	The number of attachments to a document.
<b>FILEEXT</b>	XLS	The file extension of a document.
<b>FILENAME</b>	Document Name.xls	The file name of a document.
<b>FILESIZE</b>	Numeric	The file size of a document (including embedded attachments).
<b>HASH</b>		The MD5 or SHA-1 Hash value or "de-duplication key" assigned to a document. The same hash method (MD5 or SHA-1) should be used throughout production.
<b>REDACTED</b>	YES or Blank	If a document contains a redaction, this field will display 'YES'.
<b>NATIVELINK</b>	D:\NATIVES\ABC000001.xls	The full path to a native copy of a document.
<b>FULLTEXT</b>	D:\TEXT\ABC000001.txt	The path to the full extracted text of the document. There should be a folder on the deliverable, containing a separate text file per document. These text files should be named with their corresponding bates numbers. <b>Note:</b> E-mails should include header information: author, recipient, cc, bcc, date, subject, etc. If the attachment or e-file does not extract any text, then OCR for the document should be provided.

AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED  
INFORMATION AND [PROPOSED] ORDER -11-